

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-090038
 (43)Date of publication of application : 31.03.2000

(51)Int.Cl. G06F 13/00
 G06F 15/00

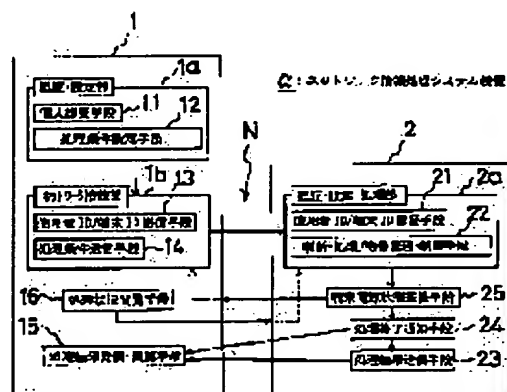
(21)Application number : 10-256840 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
 (22)Date of filing : 10.09.1998 (72)Inventor : TANAKA KEIJI
 TATEMACHI HIDETOSHI
 ISOMURA YOSHINORI
 KATO KIKUJI
 SAKAI SHIGENOBU
 SAITO TAKASHI
 ICHINOSE SUSUMU

(54) NETWORK INFORMATION PROCESSING METHOD AND SYSTEM DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance the easy portability and the information processing environment by providing a portable terminal with a recognizing function for the user, a process result display function, etc., and also providing an agent server with all information processing functions.

SOLUTION: When the portable terminal 1 receives network information service, an individual authenticating means 11 of an authentication and setting part 1a authenticates an individual who is to receive the service and its process conditions are set by a process condition setting part 12. Then a network connection part 1b sends the user ID and terminal ID to an agent server 2 by a transmitting means 13 through a public telephone network N. An authentication, setting, and processing part 2a of the server 2 specifies and authenticates the user and terminal by an ID authenticating means 21 according to stored data, and a judgement and processing/device managing and control means 22 of the server 2 grasps the requested processing contents and performs necessary processing. Then the terminal 1 once receiving the process result from a transmitting means 23 of the server 2 enables it to be browsed through a receiving and browsing means 15.



LEGAL STATUS

[Date of request for examination] 25.01.2001
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-90038
(P2000-90038A)

(43) 公開日 平成12年3月31日 (2000.3.31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 Z 5 B 0 8 5
15/00	3 1 0	15/00	3 1 0 B 5 B 0 8 9

審査請求 未請求 請求項の数38 O L (全 17 頁)

(21) 出願番号 特願平10-256840

(22) 出願日 平成10年9月10日 (1998.9.10)

(71) 出願人 000004226

日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72) 発明者 田中 敬二

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 立道 英俊

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100071113

弁理士 菅 隆彦

最終頁に続く

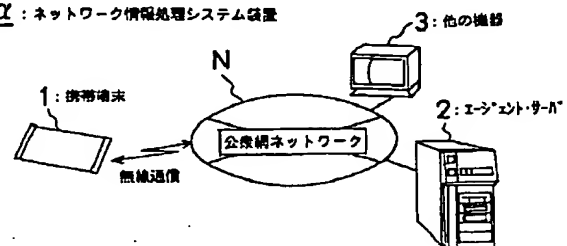
(54) 【発明の名称】 ネットワーク情報処理方法及びシステム装置

(57) 【要約】

【課題】 モバイル環境に適応した小型軽量の携帯端末を用いて高度な情報処理を行うことが可能なネットワーク情報処理方法及びシステム装置の提供。

【解決手段】 携帯端末1に、当該携帯端末1の利用者を認証する個人認証手段11と、エージェント・サーバ2における処理条件を設定する処理条件設定手段12と、IDをエージェント・サーバ2に送信するID送信手段13と、処理条件をエージェント・サーバ2に送信する処理条件送信手段14と、処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段15とを具備させ、エージェント・サーバ2に、IDを認証するID認証手段21と、所要の判断及び処理並びに公衆網ネットワークNに接続された他の機器3の管理及び制御を行う判断・処理／機器管理・制御手段22と、処理結果を携帯端末1の処理結果受信・閲覧手段15に送信する処理結果送信手段23とを具備させてなる特徴。

α: ネットワーク情報処理システム装置



【特許請求の範囲】

【請求項1】公衆網ネットワークに随時に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、

前記携帯端末に使用者の認証機能と処理結果表示機能を少なくとも持たせるとともに情報処理機能はすべて前記エージェント・サーバ側に持たせて簡易携帯性を高め情報処理環境の充実を計る、

ことを特徴とするネットワーク情報処理方法。

【請求項2】前記情報処理機能は、

前記エージェント・サーバ自身で賄う、

ことを特徴とする請求項1に記載のネットワーク情報処理方法。

【請求項3】前記情報処理機能は、

前記エージェント・サーバによる自分のホームサーバの起動を通して賄う、

ことを特徴とする請求項1に記載のネットワーク情報処理方法。

【請求項4】前記情報処理機能は、

前記エージェント・サーバ自身と自分のホームサーバの起動を通してその組合せで賄う、

ことを特徴とする請求項1に記載のネットワーク情報処理方法。

【請求項5】公衆網ネットワークに随意に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、

前記携帯端末は、

事前に登録された個人認証用照合データによる当該携帯端末の使用者の認証と、前記エージェント・サーバにおいて必要とされる処理条件の設定と、前記エージェント・サーバにおける処理結果の受信及び閲覧とを限定的に行い、

前記エージェント・サーバは、

前記携帯端末において設定された前記処理条件を元に、所要の判断及び処理並びに前記公衆網ネットワークに接続されかつ自己のホームサーバの起動を通して他の機器の管理及び制御を包括的に行う、ことを特徴とするネットワーク情報処理方法。

【請求項6】前記携帯端末は、

当該携帯端末の使用者の認証に代えて、当該携帯端末自身の認証を行う、

ことを特徴とする請求項1、2、3、4又は5に記載のネットワーク情報処理方法。

【請求項7】前記携帯端末は、

当該携帯端末の使用者の認証と、当該携帯端末自身の認証とを同時に行う、

ことを特徴とする請求項1、2、3、4、5又は6に記載のネットワーク情報処理方法。

【請求項8】前記エージェント・サーバは、

前記携帯端末において設定された前記処理条件を元に、前記公衆網ネットワークに接続された前記他の機器を当該公衆網ネットワークを介して制御し、

当該他の機器は、

前記エージェント・サーバからの制御により、当該処理条件に基づく前記所要の処理を実行する、

ことを特徴とする請求項5、6又は7に記載のネットワーク情報処理方法。

10 【請求項9】前記エージェント・サーバは、

当該エージェント・サーバにおいて得られた前記処理結果の前記携帯端末への送信に先立ち、前記所要の処理が終了した旨を示す処理終了通知を当該携帯端末に送信する、

ことを特徴とする請求項1、2、3、4、5、6、7又は8に記載のネットワーク情報処理方法。

【請求項10】前記エージェント・サーバは、

前記携帯端末における電源のオン／オフ状態を、前記公衆網ネットワークを介して監視する、

20 ことを特徴とする請求項1、2、3、4、5、6、7、8又は9に記載のネットワーク情報処理方法。

【請求項11】前記携帯端末は、

前記エージェント・サーバにおける前記所要の処理の進行状況を閲覧する、

ことを特徴とする請求項5、6、7、8、9又は10に記載のネットワーク情報処理方法。

【請求項12】前記携帯端末及び前記エージェント・サーバは、

それぞれ、前記公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う、

30 ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10又は11に記載のネットワーク情報処理方法。

【請求項13】前記エージェント・サーバは、

前記送受信データの暗号化及び復号化に際しての暗号化／復号化方式を、前記携帯端末からの要求に応じて設定する、

ことを特徴とする請求項12に記載のネットワーク情報処理方法。

40 【請求項14】前記携帯端末の使用者の認証は、

当該携帯端末に着脱可能なICカードを用いて行う、

ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12又は13に記載のネットワーク情報処理方法。

【請求項15】前記個人認証用照合データは、

前記携帯端末に着脱自在な前記ICカード自身に登録してなる、

ことを特徴とする請求項14に記載のネットワーク情報処理方法。

50 【請求項16】前記携帯端末の使用者の認証は、

パスワード入力により行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項17】前記携帯端末の使用者の認証は、
手書き文字入力により行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項18】前記携帯端末の使用者の認証は、
音声入力により行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項19】前記携帯端末の使用者の認証は、
指紋入力により行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項20】前記携帯端末の使用者の認証は、
虹彩入力により行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項21】前記携帯端末の使用者の認証は、
パスワード入力、手書き文字入力、音声入力、指紋入力
及び虹彩入力のうち2以上の入力を組み合わせて行う、
ことを特徴とする請求項1、2、3、4、5、6、7、
8、9、10、11、12、13、14又は15に記載
のネットワーク情報処理方法。

【請求項22】公衆網ネットワークに随意に接続可能な
携帯端末と、前記公衆網ネットワークに定常的に接続さ
れたエージェント・サーバとを有して構成されるネット
ワーク情報処理システム装置であって、

前記携帯端末は、
当該携帯端末の使用を許可された使用者を、事前に登録
された個人認証用照合データに基づいて認証する個人認
証手段と、前記エージェント・サーバにおいて必要とさ
れる処理条件を設定する処理条件設定手段とで構成する
認証・設定部と、

前記個人認証手段により前記使用者が適正に認証された
場合に、当該使用者に付与された使用者IDを前記エー
ジェント・サーバに送信する使用者ID送信手段と、前
記処理条件設定手段により設定された前記処理条件を前
記エージェント・サーバに送信する処理条件送信手段と
で構成するネットワーク接続部と、

前記エージェント・サーバにおける処理結果を受信して
前記使用者に閲覧させる処理結果受信・閲覧手段と、を
少なくとも具備し、

前記エージェント・サーバは、

前記携帯端末の前記使用者ID送信手段から送信された
前記使用者IDを認証する使用者ID認証手段と、この
使用者ID認証手段により前記使用者IDが適正に認証
された場合に、前記携帯端末の前記処理条件送信手段か
ら現在までに送信された前記処理条件を元に、所要の判
断及び処理並びに前記公衆網ネットワークに接続された
他の機器の管理及び制御を行う判断・処理／機器管理・
制御手段とで構成する認証・設定・処理部と、

この判断・処理／機器管理・制御手段により得られた前
記処理結果を前記携帯端末の前記処理結果受信・閲覧手
段に送信する処理結果送信手段と、を少なくとも具備す
る、

ことを特徴とするネットワーク情報処理システム装置。

【請求項23】前記ネットワーク接続部は、
前記使用者ID送信手段に代えて、
前記個人認証手段により前記使用者が適正に認証された
場合に、当該携帯端末に付与された端末IDを前記エー
ジェント・サーバに送信する端末ID送信手段を具備
し、

20 前記認証・設定・処理部は、
前記使用者ID認証手段に代えて、
前記携帯端末の当該端末ID送信手段から送信された前
記端末IDを認証する端末ID認証手段を具備し、
当該認証・設定・処理部の前記判断・処理／機器管理制
御・手段は、

前記端末ID認証手段により前記端末IDが適正に認証
された場合に、所要の判断及び処理並びに前記公衆網ネ
ットワークに接続された前記他の機器の管理及び制御を
行う機能を具備する、

30 ことを特徴とする請求項22に記載のネットワーク情報
処理システム装置。

【請求項24】前記ネットワーク接続部は、
前記個人認証手段により前記使用者が適正に認証された
場合に、前記携帯端末に付与された端末IDを前記エー
ジェント・サーバに送信する端末ID送信手段をさらに
具備し、

40 前記認証・設定・処理部は、
前記ネットワーク接続部の当該端末ID送信手段から送
信された前記端末IDを認証する端末ID認証手段をさ
らに具備し、

当該認証・設定・処理部の前記判断・処理／機器管理・
制御手段は、

前記使用者ID認証手段及び前記端末ID認証手段によ
り前記使用者ID及び前記端末IDが共に適正に認証さ
れた場合に、所要の判断及び処理並びに前記公衆網ネ
ットワークに接続された前記他の機器の管理及び制御を行
う機能をさらに具備する、ことを特徴とする請求項22
に記載のネットワーク情報処理システム装置。

50 【請求項25】前記認証・設定・処理部の前記判断・処
理／機器管理・制御手段は、

前記ネットワーク接続部の前記処理条件送信手段から送信された前記処理条件を元に、前記公衆網ネットワークに接続された前記他の機器を当該公衆網ネットワークを介して制御し、当該処理条件に基づく前記所要の処理を当該他の機器に実行させる機能を具備する、ことを特徴とする請求項22、23又は24に記載のネットワーク情報処理システム装置。

【請求項26】前記エージェント・サーバは、前記判断・処理／機器管理・制御手段により得られた前記処理結果を前記携帯端末の前記処理結果受信・閲覧手段に送信する前に、前記所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手段に送信する処理終了通知手段をさらに具備する、ことを特徴とする請求項22、23、24又は25に記載のネットワーク情報処理システム装置。

【請求項27】前記エージェント・サーバは、前記携帯端末における電源のオン／オフ状態を、前記公衆網ネットワークを介して監視する端末電源状態監視手段をさらに具備する、ことを特徴とする請求項22、23、24、25又は26に記載のネットワーク情報処理システム装置。

【請求項28】前記携帯端末は、前記エージェント・サーバにおける前記所要の処理の進行状況を閲覧する処理状況閲覧手段をさらに具備する、ことを特徴とする請求項22、23、24、25、26又は27に記載のネットワーク情報処理システム装置。

【請求項29】前記携帯端末及び前記エージェント・サーバは、それぞれ、前記公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う暗号化／復号化手段をさらに具備する、ことを特徴とする請求項22、23、24、25、26、27又は28に記載のネットワーク情報処理システム装置。

【請求項30】前記エージェント・サーバの暗号化／復号化手段は、前記携帯端末との間でネットワーク接続が完了したときに、前記送受信データの暗号化／復号化方式を規定するコードを設定して、当該コードを前記携帯端末の前記暗号化／復号化手段に送信する機能を具備し、前記携帯端末の前記暗号化／復号化手段は、前記エージェント・サーバの前記暗号化／復号化手段から送信された前記コードに対応する暗号化／復号化方式を設定する機能を具備する、ことを特徴とする請求項29に記載のネットワーク情報処理システム装置。

【請求項31】前記携帯端末は、当該携帯端末に着脱自在なICカードを含んでなり、当該ICカードは、当該携帯端末の各構成手段のうち、少なくとも前記個人

認証手段を分離装備してなる、

ことを特徴とする請求項22、23、24、25、26、27、28、29又は30に記載のネットワーク情報処理システム装置。

【請求項32】前記携帯端末に着脱自在なICカードは、前記個人認証用照合データを自身に登録する機能を具備する、

ことを特徴とする請求項31に記載のネットワーク情報処理システム装置。

【請求項33】前記個人認証手段は、前記使用者の認証を実行するためのパスワード入力機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【請求項34】前記個人認証手段は、前記使用者の認証を実行するための手書き文字入力機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【請求項35】前記個人認証手段は、前記使用者の認証を実行するための音声入力機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【請求項36】前記個人認証手段は、前記使用者の認証を実行するための指紋入力機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【請求項37】前記個人認証手段は、前記使用者の認証を実行するための虹彩入力機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【請求項38】前記個人認証手段は、前記使用者の認証を、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち2以上の入力を組み合わせ実行する機能を具備する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載のネットワーク情報処理システム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク情報

処理方法及びシステム装置に関し、詳しくは、モバイル環境において、公衆網ネットワーク上のサーバとの間でネットワーク情報サービスを授受するためのネットワーク情報処理方法、及びその実施に直接使用するネットワーク情報処理システム装置に係わる。

【0002】

【従来の技術】近年、モバイル・コンピュータなどと呼ばれる携帯端末を、アナログ電話回線やISDN回線（ISDN：サービス統合デジタル通信網）、更には携帯電話回線やPHS（Personal Handyphone System）などの公衆網からなるネットワーク（以下、単に「公衆網ネットワーク」という）に接続する。

【0003】その携帯端末の具備する通信機能を用いて、時間や場所にとらわれることなく、インターネット接続により所望の情報の検索、閲覧を行ったり、或いは、その公衆網ネットワーク上の特定のサーバに対し情報のアップロードやダウンロードを行って、自己の情報の蓄積や、他者の情報の取出し、閲覧を行えるようになっている。また、公衆網ネットワーク上の任意の情報端末との間で、電子メールの転送を容易に行えるようになっている。

【0004】以上のようなモバイル環境におけるネットワーク情報サービスの提供の仕組みは、公衆網ネットワークに接続され主にデータを保持したサーバと携帯端末との間で、所要のデータのやり取りを行うことが基本となっている。そして、このような形態のネットワーク情報サービスの発展に伴い、現在では、より一層の携帯性を重視し、当該サービスの授受に特化した小型軽量の携帯端末が開発されるに至っている。

【0005】例えば、Windows CE（“Windows”は、米マイクロソフト社登録商標）に代表される比較的規模の小さいOS（オペレーティング・システム）の搭載されたPDA（Personal Digital Assistant）などが、その好例である。

【0006】この種のPDAは、上述したネットワーク情報サービスを実現するためのアプリケーション・ソフトウェア（以下、単に「アプリケーション」という）を搭載する他、通常では、例えば、スケジュール管理機能、カレンダー機能、メモ機能などといった、モバイル環境での使用に適した必要最小限の機能を実現するための簡易なアプリケーションのみを搭載している。

【0007】なお、以上のようにネットワーク情報サービスの授受に特化したPDAの他にも、A5ファイル・サイズやB4ファイル・サイズのノート型パソコンを、携帯端末として用いる場合もある。

【0008】この種のノート型パソコンは、処理速度が比較的速く、かつ1GB相当或いはそれ以上の記憶容量を有するデータ蓄積装置を内蔵しているため、当該ノート型パソコンによれば、例えば、Windows 95や98などに代表される高度なOSのもと、表計算ソフト

ト、ワープロ・ソフト、管理ソフト、ドロー・ソフトなど、そのノート型パソコンの使用者の要求に応じた高度なアプリケーションを実行できるのは勿論のこと、所要のネットワーク情報サービスの授受を行うことも可能である。

【0009】

【発明が解決しようとする課題】ところで、上述した携帯端末のうち、ネットワーク情報サービスの授受に特化したPDAでは、その記憶容量等の関係から、例えば、表計算ソフト、ワープロ・ソフト、管理ソフト、ドロー・ソフトなどといった、高度で占有プログラム容量の大きいアプリケーションの利用が事実上困難なため、モバイル環境においては、使用できるアプリケーションの種類につき制約を受けてしまう。

【0010】また、モバイル環境に特有のアプリケーションとして、例えば、携帯端末の使用者の地図上の存在位置を、GPS衛星（GPS：Global Positioning System）からの電波を利用して当該携帯端末の画面上に表示し、所望により、使用者がこれから向かおうとしている目的地までの経路をリアル・タイムに案内表示する、いわゆるナビゲーション・ソフトなどの利用が考えられる。

【0011】この種のソフトにあっては、携帯端末の使用者の移動に伴って逐次変化する位置情報に対応するために、所定の地理範囲（例えば日本全土）の全地域に及ぶ地図データを端末上に備えておく必要があり、これをPDAにより行うことは、前述の記憶容量等の関係から実際上不可能である。

【0012】これに対し、ノート型パソコンを携帯端末として用いた場合、上述のPDAにおける場合のような不都合を生じることはないが、ノート型パソコンは、PDAに比べ寸法が大きく重量もあるため、本来、携帯に適するとは言いがたい面がある。

【0013】また昨今では、急激な技術発達に伴い、ノート型パソコンの処理速度が飛躍的に向上すると共に、内蔵されるデータ蓄積装置の単位体積あたりの記憶容量も大幅に増加しているため、実際上の問題として、例えば、わずか1年前に入手したノート型パソコンのハードウェア・スペックが、現在に至り、もはや陳腐化したものとなるなどの状況を生じている。

【0014】こうした状況のもと、ノート型パソコン上で実行されるアプリケーションの規模（プログラム容量）も年々増大する傾向にあるため、旧型（例えば、上述した1年前）のノート型パソコンでは、そのハードウェア・スペック上の制約から、こうした最新のアプリケーション（例えば、前述したナビゲーション・ソフトなど）を実行できないこともある。このようなハードウェア・スペックの陳腐化に起因する問題は、将来的にも、今後しばらくの間は続くものと予想される。

【0015】ここにおいて、本発明の主要な目的は次の

10

20

30

40

50

とおりである。

【0016】即ち、本発明の第1の目的は、モバイル環境に適応した小型軽量の携帯端末を用いながら、公衆網ネットワークを通じ高度な情報処理を行うことの可能なネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【0017】本発明の第2の目的は、高度で占有プログラム容量の大きい様々なアプリケーションを随意に選択使用することの可能なネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【0018】本発明の第3の目的は、使用する携帯端末のハードウェア・スペックにつき、将来にわたり陳腐化の問題の生じることのないネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【0019】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0020】

【課題を解決するための手段】本発明方法においては、携帯端末に、当該携帯端末の使用者の認証、エージェント・サーバにおける処理条件の設定、エージェント・サーバにおける処理結果の受信及び閲覧などの処理を限定的に行わせ、エージェント、サーバには、携帯端末において設定された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を包括的行わせる、という手法を講じる特徴を有する。

【0021】また、本発明システム装置においては、携帯端末に、当該携帯端末の使用者を認証する個人認証手段と、エージェント・サーバにおける処理条件を設定する処理条件設定手段と、使用者及び／又は携帯端末に付与されたID（識別子）をエージェント・サーバに送信するID送信手段と、処理条件をエージェント・サーバに送信する処理条件送信手段と、処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段とを具備させ、エージェント・サーバには、IDを認証するID認証手段と、現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う判断・処理／機器管理・制御手段と、処理結果を携帯端末の処理結果受信・閲覧手段に送信する処理結果送信手段とを具備させる、という手法を講じる特徴を有する。

【0022】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法を採用することにより、前記目的を達成するよう為される。

【0023】即ち、本発明方法の第1の特徴は、公衆網ネットワークに随時に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、前

記携帯端末に使用者の認証機能と処理結果表示機能を少なくとも持たせるとともに情報処理機能はすべて前記エージェント・サーバ側に持たせて簡易携帯性を高め情報処理環境の充実を計ってなるネットワーク情報処理方法の構成採用にある。

【0024】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における前記情報処理機能が、前記エージェント・サーバ自身で賄ってなるネットワーク情報処理方法の構成採用にある。

10 【0025】本発明方法の第3の特徴は、上記本発明方法の第1の特徴における前記情報処理機能が、前記エージェント・サーバによる自分のホームサーバの起動を通して賄ってなるネットワーク情報処理方法の構成採用にある。

【0026】本発明方法の第4の特徴は、上記本発明方法の第1の特徴における前記情報処理機能が、前記エージェント・サーバ自身と自分のホームサーバの起動を通してその組合せで賄ってなるネットワーク情報処理方法の構成採用にある。

20 【0027】本発明方法の第5の特徴は、公衆網ネットワークに随意に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、携帯端末が、事前に登録された個人認証用照合データによる当該携帯端末の使用者の認証と、エージェント・サーバにおいて必要とされる処理条件の設定と、エージェント・サーバにおける処理結果の受信及び閲覧とを限定的に行い、エージェント・サーバが、携帯端末において設定された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続されかつ自己のホームサーバの起動を通して他の機器の管理及び制御を包括的に行ってなるネットワーク情報処理方法の構成採用にある。

【0028】本発明方法の第6の特徴は、上記本発明方法の第1、第2、第3、第4又は第5の特徴における携帯端末が、当該携帯端末の使用者の認証に代えて、当該携帯端末自身の認証を行ってなるネットワーク情報処理方法の構成採用にある。

30 【0029】本発明方法の第7の特徴は、上記本発明方法の第1、第2、第3、第4、第5又は第6の特徴における携帯端末が、当該携帯端末の使用者の認証と、当該携帯端末自身の認証とを同時に行ってなるネットワーク情報処理方法の構成採用にある。

【0030】本発明方法の第8の特徴は、上記本発明方法の第5、第6又は第7の特徴におけるエージェント・サーバが、携帯端末において設定された処理条件を元に、公衆網ネットワークに接続された他の機器を当該公衆網ネットワークを介して制御し、当該他の機器が、エージェント・サーバからの制御により、当該処理条件に基づく所要の処理を実行してなるネットワーク情報処理方法の構成採用にある。

【0031】本発明方法の第9の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7又は第8の特徴におけるエージェント・サーバが、当該エージェント・サーバにおいて得られた処理結果の携帯端末への送信に先立ち、所要の処理が終了した旨を示す処理終了通知を当該携帯端末に送信してなるネットワーク情報処理方法の構成採用にある。

【0032】本発明方法の第10の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8及び第9の特徴におけるエージェント・サーバが、携帯端末における電源のオン／オフ状態を、公衆網ネットワークを介して監視してなるネットワーク情報処理方法の構成採用にある。

【0033】本発明方法の第11の特徴は、上記本発明方法の第5、第6、第7、第8、第9又は第10の特徴における携帯端末が、エージェント・サーバにおける所要の処理の進行状況を閲覧してなるネットワーク情報処理方法の構成採用にある。

【0034】本発明方法の第12の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における携帯端末及びエージェント・サーバが、それぞれ、公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行ってなるネットワーク情報処理方法の構成採用にある。

【0035】本発明方法の第13の特徴は、上記本発明方法の第12の特徴におけるエージェント・サーバが、送受信データの暗号化及び復号化に際しての暗号化／復号化方式を、携帯端末からの要求に応じて設定してなるネットワーク情報処理方法の構成採用にある。

【0036】本発明方法の第14の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12又は第13の特徴における携帯端末の使用者の認証が、当該携帯端末に着脱可能なICカードを用いて行ってなるネットワーク情報処理方法の構成採用にある。

【0037】本発明方法の第15の特徴は、上記本発明方法の第14の特徴における個人認証用照合データが、前記携帯端末に着脱自在なICカード自身に登録してなるネットワーク情報処理方法の構成採用にある。

【0038】本発明方法の第16の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、パスワード入力により行ってなるネットワーク情報処理方法の構成採用にある。

【0039】本発明方法の第17の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、手

書き文字入力により行ってなるネットワーク情報処理方法の構成採用にある。

【0040】本発明方法の第18の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、音声入力により行ってなるネットワーク情報処理方法の構成採用にある。

【0041】本発明方法の第19の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、指紋入力により行ってなるネットワーク情報処理方法の構成採用にある。

【0042】本発明方法の第20の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、虹彩入力により行ってなるネットワーク情報処理方法の構成採用にある。

【0043】本発明方法の第21の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における携帯端末の使用者の認証が、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち2以上の入力を組み合わせて行ってなるネットワーク情報処理方法の構成採用にある。

【0044】一方、本発明装置の第1の特徴は、公衆網ネットワークに随意に接続可能な携帯端末と、公衆網ネットワークに定常的に接続されたエージェント・サーバとを有して構成されるネットワーク情報処理システム装置であって、携帯端末は、当該携帯端末の使用を許可された使用者を、事前に登録された個人認証用照合データに基づいて認証する個人認証手段と、エージェント・サーバにおいて必要とされる処理条件を設定する処理条件設定手段とで構成する認証・設定部と、個人認証手段により使用者が適正に認証された場合に、当該使用者に付与された使用者IDをエージェント・サーバに送信する使用者ID送信手段と、処理条件設定手段により設定された処理条件をエージェント・サーバに送信する処理条件送信手段とで構成するネットワーク接続部と、エージェント・サーバにおける処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段と、を少なくとも具備し、エージェント・サーバは、携帯端末の使用者ID送信手段から送信された使用者IDを認証する使用者ID認証手段と、この使用者ID認証手段により使用者IDが適正に認証された場合に、携帯端末の処理条件送信手段から現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う判断・処理／機器管理・制御

13

手段とて構成する認証・設定・処理部と、この判断・処理／機器管理・制御手段により得られた処理結果を携帯端末の処理結果受信・閲覧手段に送信する処理結果送信手段と、を少なくとも具備してなるネットワーク情報処理システム装置の構成採用にある。

【0045】本発明装置の第2の特徴は、上記本発明装置の第1の特徴におけるネットワーク接続部が、使用者ID送信手段に代えて、個人認証手段により使用者が適正に認証された場合に、当該携帯端末に付与された端末IDをエージェント・サーバに送信する端末ID送信手段を具備し、認証・設定・処理部が、使用者ID認証手段に代えて、携帯端末の当該端末ID送信手段から送信された端末IDを認証する端末ID認証手段を具備し、当該認証・設定・処理部の判断・処理／機器管理制御・手段が、端末ID認証手段により端末IDが適正に認証された場合に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0046】本発明装置の第3の特徴は、上記本発明装置の第1の特徴におけるネットワーク接続部が、個人認証手段により使用者が適正に認証された場合に、携帯端末に付与された端末IDをエージェント・サーバに送信する端末ID送信手段をさらに具備し、認証・設定・処理部が、ネットワーク接続部の当該端末ID送信手段から送信された端末IDを認証する端末ID認証手段をさらに具備し、当該認証・設定・処理部の判断・処理／機器管理・制御手段が、使用者ID認証手段及び端末ID認証手段により使用者ID及び端末IDが共に適正に認証された場合に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う機能をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【0047】本発明装置の第4の特徴は、上記本発明装置の第1、第2又は第3の特徴における認証・設定・処理部の判断・処理／機器管理・制御手段が、ネットワーク接続部の処理条件送信手段から送信された処理条件を元に、公衆網ネットワークに接続された他の機器を当該公衆網ネットワークを介して制御し、当該処理条件に基づく所要の処理を当該他の機器に実行させる機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0048】本発明装置の第5の特徴は、上記本発明装置の第1、第2、第3又は第4の特徴におけるエージェント・サーバが、判断・処理／機器管理・制御手段により得られた処理結果を携帯端末の処理結果受信・閲覧手段に送信する前に、所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手段に送信する処理終了通知手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

14

【0049】本発明装置の第6の特徴は、上記本発明装置の第1、第2、第3、第4又は第5の特徴におけるエージェント・サーバが、携帯端末の電源のオン／オフ状態を、公衆網ネットワークを介して監視する端末電源状態監視手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【0050】本発明装置の第7の特徴は、上記本発明装置の第1、第2、第3、第4、第5又は第6の特徴における携帯端末が、エージェント・サーバにおける所要の処理の進行状況を閲覧する処理状況閲覧手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【0051】本発明装置の第8の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6又は第7の特徴における携帯端末及びエージェント・サーバが、それぞれ、公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う暗号化／復号化手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【0052】本発明装置の第9の特徴は、上記本発明装置の第8の特徴におけるエージェント・サーバの暗号化／復号化手段が、携帯端末との間でネットワーク接続が完了したときに、送受信データの暗号化／復号化方式を規定するコードを設定して、当該コードを携帯端末の暗号化／復号化手段に送信する機能を具備し、携帯端末の暗号化／復号化手段が、エージェント・サーバの暗号化／復号化手段から送信されたコードに対応する暗号化／復号化方式を設定する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0053】本発明装置の第10の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8又は第9の特徴における携帯端末が、当該携帯端末に着脱自在なICカードを含んでなり、当該ICカードが、当該携帯端末の各構成手段のうち、少なくとも個人認証手段を分離装備してなるネットワーク情報処理システム装置の構成採用にある。

【0054】本発明装置の第11の特徴は、上記本発明装置の第10の特徴における携帯端末に着脱自在なICカードが、個人認証用照合データを自身に登録する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0055】本発明装置の第12の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手段が、使用者の認証を実行するためのパスワード入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0056】本発明装置の第13の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手

段が、使用者の認証を実行するための手書き文字入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0057】本発明装置の第14の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手段が、使用者の認証を実行するための音声入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0058】本発明装置の第15の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手段が、使用者の認証を実行するための指紋入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0059】本発明装置の第16の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手段が、使用者の認証を実行するための虹彩入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0060】本発明装置の第17の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における個人認証手段が、使用者の認証を、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち2以上の入力を組み合わせ実行する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【0061】

【発明の実施の形態】以下、添付図面を参照しつつ、本発明の実施の形態を、その第1及び第2装置例及びこれらに対応する第1及び第2方法例につき説明する。

【0062】(第1装置例)図1は、本装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。また、図2は、本装置例に係るネットワーク情報処理システム装置における携帯端末及びエージェント・サーバの機能構成を示すブロック図である。

【0063】まず、図1に示すように、この第1装置例に係るネットワーク情報処理システム装置αは、基本的に、公衆網ネットワークNに随意に接続可能な携帯端末1と、公衆網ネットワークに定常的に接続されたエージェント・サーバ2とを有して構成され、これらに加え、公衆網ネットワークNには、会社や家庭に設置されたパソコンなどの情報端末や、或いは、情報端末として機能するテレビ受像機などの他の機器3が接続できるようにになっている。

【0064】なお、公衆網ネットワークNと携帯端末1との接続形態は任意であるが、この第1装置例では、無線通信を用いる携帯電話回線やPHSなどによって、所要のネットワーク接続を行った例を示している。

【0065】次に、図2に示すように、携帯端末1は、基本的に、当該携帯端末1の使用を許可された使用者を、事前に登録された個人認証用照合データに基づいて認証する個人認証手段11と、エージェント・サーバ2において必要とされる処理条件を設定する処理条件設定手段12とからなる認証・設定部1aと、個人認証手段11により使用者が適正に認証された場合に、当該使用者に付与された使用者ID及び/又は携帯端末1に付与された端末IDをエージェント・サーバ2に送信する使用者ID/端末ID送信手段13と、処理条件設定手段12により設定された処理条件をエージェント・サーバ2に送信する処理条件送信手段14とからなるネットワーク接続部1bと、エージェント・サーバ2における処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段15とを具備して構成される。

【0066】なお、上述の個人認証手段11としては、所要の使用者の認証を、例えば、パスワード入力により行うもの、手書き文字入力により行うもの、音声入力により行うもの、指紋入力により行うもの、虹彩入力により行うものなどが挙げられるが、その適用に際しては、これら各入力を単独で用いたり、或いは、2以上の入力を組み合わせて用いるようにしてもよい。

【0067】また、携帯端末1には、以上の各手段他、エージェント・サーバ2における所要の処理の進行状況を検査する処理状況閲覧手段16を具備させてもよい。

【0068】一方、エージェント・サーバ2は、基本的に、携帯端末1の使用者ID/端末ID送信手段13から送信された使用者ID及び/又は端末IDを認証する使用者ID/端末ID認証手段21と、この使用者ID/端末ID認証手段21により使用者ID及び/又は端末IDが適正に認証された場合に、携帯端末1の処理条件送信手段12から現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークNに接続されかつ自分のホームサーバの起動を通して他の機器3の管理及び制御を行う判断・処理/機器管理・制御手段22とからなる認証・設定・処理部2aと、この判断・処理/機器管理・制御手段22により得られた処理結果を携帯端末1の処理結果受信・閲覧手段15に送信する処理結果送信手段23とを具備して構成される。

【0069】なお、判断・処理/機器管理・制御手段22は、携帯端末1の処理条件送信手段14から送信された処理条件を元に、公衆網ネットワークNに接続された他の機器3を当該公衆網ネットワークNを介して制御し、当該処理条件に基づく所要の処理を当該他の機器3に実行させることも可能である。

【0070】また、エージェント・サーバ2に対して、以上の各手段の他、判断・処理/機器管理・制御手段21により得られた処理結果を携帯端末1の処理結果受信・閲覧手段15に送信する前に、所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手

段15に送信する処理終了通知手段24を具備させたり、或いは、携帯端末1の電源のオン/オフ状態を、公衆網ネットワークNを介して監視する端末電源状態監視手段25を具備させてもよい。

【0071】さらに、携帯端末1及びエージェント・サーバ2の両者には、それぞれ、公衆網ネットワークNを介し双方向でやり取りされる送受信データの暗号化及び復号化を行う暗号化/復号化手段(図示せず)を具備させてもよい。

【0072】ここで、エージェント・サーバ2の暗号化/復号化手段には、携帯端末1との間でネットワーク接続が完了したときに、送受信データの暗号化/復号化方式を規定するコードを設定させて、当該コードを携帯端末1の暗号化/復号化手段に送信させ、これに対し、携帯端末1の暗号化/復号化手段には、エージェント・サーバ2の暗号化/復号化手段から送信されたコードに対応する暗号化/復号化方式を設定させるようにすればよい。

【0073】(第1方法例)次に、以上のように構成された第1装置例に係るネットワーク情報処理システム装置αに適用される第1方法例につき説明する。

【0074】まず、携帯端末1においてネットワーク情報サービスを授受するために、当該携帯端末1の認証・設定部1aにおいては、例えば、指紋認証装置(図示せず)などの個人認証手段11により、当該サービスを受けようとする個人を認証し、当該サービスを受けるためのエージェント・サーバ2における処理条件を、処理条件設定手段12により設定する。

【0075】その後、携帯端末1のネットワーク接続部1bは、エージェント・サーバ2との間で公衆網ネットワークNを介したネットワーク接続を行い、使用者ID及び/又は端末IDを、使用者ID/端末ID送信手段13によってエージェント・サーバ2に送信することにより、当該エージェント・サーバ2の認証・設定・処理部2aにおいては、自己の管理している過去の蓄積データを元に、使用者ID/端末ID認証手段21において使用者及び/又は携帯端末を特定して認証することができ、これによりネットワーク情報サービスの提供の可否が判断される。

【0076】そして、このようにしてネットワーク情報サービスの提供が許容されると、携帯端末1のネットワーク接続部1bは、エージェント・サーバ2における処理条件を、処理条件送信手段14によって送信し、これを受信した当該エージェント・サーバ2の認証・設定・処理部2aにおける判断・処理/機器管理・制御手段22は、携帯端末1から要求されている処理内容を把握して、判断、設定、処理、管理、或いは、他の機器3を制御するようにとの各種命令に対する所要の処理を実行する。

【0077】なお、携帯端末1においては、エージェン

ト・サーバ2の処理結果送信手段23により、当該エージェント・サーバ2における処理結果を通信で受け取ることができ、さらに処理結果受信・閲覧手段15により、その処理結果を閲覧することができる。

【0078】そして、このような一連の処理が、ネットワーク情報処理システム装置α内で行われることにより、高度な処理プログラムが動作しない軽微な携帯端末1であっても、高度な処理結果を得ることが可能となる。

【0079】なお、エージェント・サーバ2に処理終了通知手段24を具備させることにより、携帯端末1の利用者は、処理結果受信・閲覧手段15により、エージェント・サーバ2における所要の処理が終了したことを瞬時に知ることができ、この処理終了通知手段24により、一層利用しやすいネットワーク情報処理システム装置αを構築することができる。

【0080】この処理終了通知手段24の動作につき、具体的には、エージェント・サーバ2が携帯端末1から処理を依頼された場合に、当該携帯端末1から端末IDを受け取って、その携帯端末1を認識した後に所要の処理を実行するようにし、その処理が終了した時点で、認識した携帯端末1の端末IDを元に、その携帯端末1に対し終了通知を発信するようにするとよい。

【0081】また、エージェント・サーバ2に端末電源状態監視手段25を具備させることにより、携帯端末1の電源がオフ状態のときに、不要な処理終了通知を送信しなくても済むようになるメリットがある。

【0082】この端末電源状態監視手段25の動作につき、具体的には、携帯端末1の電源がオン状態となっており、端末IDなど当該携帯端末1を特定できる情報を含んだ電波を、その携帯端末1に連続的又は断続的に発信させておき、この電波を、無線基地局(図示せず)から公衆網ネットワークNを介してエージェント・サーバ2に送信することにより、当該携帯端末1の電源のオン/オフ状態を監視させるようにするとよい。

【0083】さらに、携帯端末1に処理状況閲覧手段16を具備させることにより、エージェント・サーバ2において実行中の処理の終了に時間がかかるものと見込まれる場合に、その処理が終了する前に、当該処理の変更(強制終了など)を行うことができるなどのメリットがある。

【0084】この処理状況閲覧手段16の動作につき、具体的には、携帯端末1から処理状況確認メッセージが無線により送信させて、そのメッセージを受け取ったエージェント・サーバ2に、そのときの処理状況を携帯端末1に送信させるようにするとよい。

【0085】さらにまた、携帯端末1及びエージェント・サーバ2の両者に暗号化/復号化手段を具備させることにより、双方向の送受信データが第三者に不正に受信されて利用されるのを、防止できるメリットがある。

【0086】(第2装置例) 続いて、図3は、本装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【0087】同図に示すように、この本装置例に係るネットワーク情報処理システム装置は、前記第1装置例におけるそれと同様、基本的に、公衆網ネットワークNに随意に接続可能な携帯端末1と、公衆網ネットワークに定常的に接続されたエージェント・サーバ2とを有して構成され、携帯端末1が、当該端末に着脱自在なICカード4を含んでなり、当該ICカード4が、携帯端末1の構成手段に含まれる個人認証手段11を分離装備すると共に、個人認証用照合データを自身に登録したものとなっている。

【0088】また、このICカード4は、公衆網ネットワークNに接続された他の端末5に対しても装着自在に構成することが可能である。(ICカード4自身の構成については、本願出願人による特願平10-144885号に詳しい。)

【0089】(第2方法例) 次に、以上のように構成された第2装置例に係るネットワーク情報処理システム装置に適用される第2方法例につき説明する。

【0090】個人認証をICカード4により行う場合、当該ICカード4には、個人認証用照合データは勿論、個人が受けられるネットワーク情報サービスの種類に関するデータを保存しておくようにする。

【0091】このICカード4を用いたネットワーク情報処理システム装置においては、携帯端末1における個人認証がICカード4内のデータに基づいて行われる以外は、図2のブロック図に示した各構成手段により実現される機能と同様な機能を有するが、当該ICカード4によって、個人認証とネットワーク情報サービスの設定が行えるようになるため、図示の他の端末5を用いて、同様に高度なネットワーク情報サービスを受けようとする場合、そのICカード4のみを持ち運べば済むというメリットがある。

【0092】また、このICカード4に、例えば指紋認証装置などの個人認証手段11を、携帯端末1とは独立して具備させることにより、当該携帯端末1における個人認証処理が不要となって、その携帯端末1の装備を、一層軽微にすることができるというメリットがある。

【0093】

【実施例】 続いて、実施例として、本実施形態を利用してネットワーク情報サービスを受ける場合の一連の手順について説明する。

【0094】本発明によりネットワーク情報サービスを受けるためには、携帯端末1の利用者が、利用したいサービスの種類をエージェント・サーバ2を保有するプロバイダ(図示せず)に申請し、当該サービスを新規に登録するための「サービス新規登録」と、携帯端末1の利用者が、既に利用登録済みのサービスの利用環境を設定

し、そのときの設定情報をプロバイダに通知するための「サービス環境設定」とを行い、その後、実際の「サービス利用」が可能となる。

【0095】以下、これら各フローを、第1装置例及びこれに適用する第1方法例における場合(ICカード不要)と、並びに第2装置例及びこれに適用する第2方法例における場合(ICカード要)とにつき順に説明する。

【0096】<ICカード不要のサービス新規登録>図4は、ICカード不要のサービス新規登録の手順を説明するためのフローチャートである。

【0097】ICカード4不要のサービス新規登録に際しては、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求して(ST1)、当該使用者IDの投入後にローカル個人認証を行う(ST2)。

【0098】ここで、投入された使用者IDが適正なものであるか否かを判定するが(ST3)、それが、既に携帯端末1に登録されているユーザ情報と一致しない場合(ST3; NO)、携帯端末1は、ローカル個人認証が失敗したとして、当該携帯端末1の利用者に対し登録不可通知を提示して(ST4)、処理を終了する。

【0099】これに対し、投入された使用者IDが携帯端末1に登録されているユーザ情報と一致した場合(ST3; YES)には、携帯端末1は、エージェント・サーバ2に対し当該使用者IDを送信し(ST5)、以下、当該エージェント・サーバ2において、その使用者IDのチェックを行って(ST6)、これが適正な使用者IDであるか否かを判定する(ST7)。

【0100】この判定の結果、送信されてきた使用者IDが不適正なものである場合(ST7; NO)には、新規サービスの利用が不可であるとして、前述のST4の処理において、当該携帯端末1の利用者に対し登録不可通知を提示して処理を終了するが、それが適正なものである場合(ST7; YES)、エージェント・サーバ2は、新規サービスの利用が可能であるとして、当該新規サービスに対する利用者IDを登録し(ST8)、以下、携帯端末1に、その登録が完了した旨を通知すると共に(ST9)、当該携帯端末1において所要のサービスIDを記入して(ST10)、全ての処理を終了する。

【0101】<ICカード不要のサービス環境設定>図5は、ICカード不要のサービス環境設定の手順を説明するためのフローチャートである。

【0102】ICカード4不要のサービス環境設定に際しては、上述のサービス新規登録と同様に、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求して(ST11)、当該使用者IDの投入後にローカル個人認証を行う(ST12)。

【0103】ここで、投入された使用者IDが適正なものであるか否かを判定するが(ST13)、それが、既

21

に携帯端末1に登録されているユーザ情報と一致しない場合（ST13；NO）、携帯端末1は、上述のサービス新規登録と同様、ローカル個人認証が失敗したとして、当該携帯端末1の利用者に対し登録不可通知を提示して（ST14）、処理を終了する。

【0104】これに対し、投入された使用者IDが携帯端末1に登録されているユーザ情報と一致した場合（ST13；YES）には、携帯端末1は、所要のサービス利用環境の設定を行った後に（ST15）、エージェント・サーバ2に対し、使用者IDと当該サービス利用環境を送信し（ST16）、以下、当該エージェント・サーバ2において、そのサービス利用環境のチェックを行って（ST17）、これが適正なサービス利用環境であるか否かを判定する（ST18）。

【0105】この判定の結果、送信されてきたサービス利用環境が不適正なものである場合（ST18；NO）には、前述のST14の処理において、当該携帯端末1の利用者に対し登録不可通知を提示して処理を終了するが、それが適正なものである場合（ST18；YES）、エージェント・サーバ2は、サービス利用環境の設定登録を行って（ST19）、携帯端末1に、その設定登録が完了した旨を通知すると共に（ST20）、当該携帯端末1において所要のサービス利用環境データを書き込んで（ST21）、全ての処理を終了する。

【0106】＜ICカード不要のサービス利用＞図6及び図7は、ICカード不要のサービス利用のそれぞれ前半及び後半の手順を説明するためのフローチャートである。なお、本図では、携帯端末1の使用者の位置情報をエージェント・サーバ2が捕捉し、当該使用者の現在位置を表した周辺地図を携帯端末1へ転送するサービスの利用について説明する。

【0107】ICカード4不要のサービス利用（進路ナビゲーション・サービス）に際しては、上述のサービス新規登録及び環境設定と同様に、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求して（ST31）、当該使用者IDの投入後にローカル個人認証を行う（ST32）。

【0108】ここで、投入された使用者IDが適正なものであるか否かを判定するが（ST33）、それが、既に携帯端末1に登録されているユーザ情報と一致しない場合（ST33；NO）、携帯端末1は、上述のサービス新規登録及び環境設定と同様、ローカル個人認証が失敗したとして、当該携帯端末1の利用者に対し登録不可通知を提示して（ST34）、処理を終了する。

【0109】これに対し、投入された使用者IDが携帯端末1に登録されているユーザ情報と一致した場合（ST33；YES）には、携帯端末1は、エージェント・サーバ2に対し、当該使用者IDと、前述のサービス新規登録の処理で携帯端末1に記入したサービスIDとを送信し（ST35）、以下、当該エージェント・サーバ

22

2において、その使用者ID及びサービスIDのチェックを行って（ST36）、これが適正なサービス利用環境であるか否かを判定する（ST37）。

【0110】この判定の結果、送信されてきた使用者ID及びサービスIDが不適正なものである場合（ST37；NO）には、前述のST34の処理において、当該携帯端末1の利用者に対しサービス不可通知を提示して処理を終了するが、それらが適正なものである場合（ST37；YES）には、携帯端末1の使用者へのサービス許可通知及び待機要求を行う（ST38）。なお、このとき携帯端末1は、通信待ち受け状態となっている。

【0111】その後、エージェント・サーバ2では、携帯端末1の使用者の位置情報を捕捉し（ST39）、例えば、携帯端末1の使用者の現在位置を表した地図情報を作成するなどといった出力情報処理を行った後に（ST40）、その携帯端末1に対し処理終了通知を送信する（ST41）。

【0112】これに対し、携帯端末1では、送信されてきた処理終了通知を表示し（ST42）、再びローカル個人認証を行う（ST43）。

【0113】ここで、再び投入された使用者IDが適正なものであるか否かを判別するが（ST44）、それが、これまでに携帯端末1に登録されているユーザ情報と一致しない場合（ST44；NO）、携帯端末1は、その使用者から誤った使用者IDが入力されたとして、再び、当該携帯端末1の利用者に対し個人認証を要求して（ST45）、前述のST43のローカル個人認証を繰り返す行。

【0114】これに対し、投入された使用者IDが携帯端末1に登録されているユーザ情報と一致した場合（ST44；YES）、エージェント・サーバ2は、携帯端末1に対し処理結果を送信し（ST46）、以下、携帯端末1においては、当該処理結果の受信・閲覧表示を行った後に（ST47）、エージェント・サーバ2に受信完了通知を送信し（ST48）、これにより全ての処理を終了する。

【0115】続いて、ICカード4を使用したときのサービス提供について説明する。

【0116】＜ICカード要のサービス新規登録＞図8は、ICカード要のサービス新規登録の手順を説明するためのフローチャートである。

【0117】ICカード4要のサービス新規登録に際しては、その未使用時における場合と同様、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求するが（ST51）、当該使用者IDの投入後のローカル個人認証（ST52）及びその使用者IDの判定（ST53）は、携帯端末1ではなく、ICカード4において行う。

【0118】そして、再び携帯端末1において、投入された使用者IDがユーザ情報と一致しない場合（ST5

10

20

30

40

50

3; NO)には、当該携帯端末1の利用者に対し登録不可通知を提示し(ST54)、一致した場合(ST53; YES)には、エージェント・サーバ2に対し当該使用者IDを送信し(ST55)、以下、当該エージェント・サーバ2において、使用者IDのチェック(ST56)及びその判定(ST57)を行う。

【0119】以下、同様に、送信されてきた使用者IDが不適正なものである場合(ST57; NO)には、携帯端末1の利用者に対し登録不可通知を提示し、それが適正なものである場合(ST57; YES)には、エージェント・サーバ2は、新規サービスに対する利用者IDを登録し(ST58)、さらに、携帯端末1に、その登録が完了した旨を通知する(ST59)。

【0120】そして、以上の処理の終了と共に、携帯端末1の制御の下、ICカード4に所要のサービスIDを記入し(ST60)、これにより全ての処理を終了する。

【0121】<ICカード要のサービス環境設定>図9は、ICカード要のサービス環境設定の手順を説明するためのフローチャートである。

【0122】ICカード4要のサービス環境設定に際しては、その未使用時における場合と同様、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求する(ST61)、当該使用者IDの投入後のローカル個人認証(ST62)及びその使用者IDの判定(ST63)は、携帯端末1ではなく、ICカード4において行う。

【0123】そして、再び携帯端末1において、投入された使用者IDがユーザ情報と一致しない場合(ST63; NO)には、当該携帯端末1の利用者に対し登録不可通知を提示し(ST64)、一致した場合(ST63; YES)には、サービス利用環境の設定を行った後に(ST65)、エージェント・サーバ2に対し、使用者IDと当該サービス利用環境を送信し(ST66)、以下、当該エージェント・サーバ2において、そのサービス利用環境のチェック(ST67)及びその判定(ST68)を行う。

【0124】以下、同様に、送信されてきたサービス利用環境が不適正なものである場合(ST68; NO)には、当該携帯端末1の利用者に対し登録不可通知を提示し、それが適正なものである場合(ST68; YES)には、エージェント・サーバ2は、サービス利用環境の設定登録を行って(ST69)、携帯端末1に、その設定登録が完了した旨を通知する(ST70)。

【0125】そして、以上の処理の終了と共に、携帯端末1の制御の下、ICカード4に所要のサービス利用環境データを書き込み(ST71)、これにより全ての処理を終了する。

【0126】<ICカード要のサービス利用>図10及び図11は、ICカード要のサービス利用のそれぞれ前

半及び後半の手順を説明するためのフローチャートである。なお、本図においても、前述の進路ナビゲーション・サービスについて説明する。

【0127】ICカード4要のサービス利用に際しては、その不要の場合と同様、まず、携帯端末1から、その使用者に対して使用者IDの投入を要求する(ST81)、当該使用者IDの投入後にローカル個人認証(ST82)及びその使用者IDの判定(ST83)は、携帯端末1ではなく、ICカード4において行う。

【0128】そして、再び携帯端末1において、その使用者IDがユーザ情報と一致しない場合(ST83; NO)には、携帯端末1は、当該携帯端末1の利用者に対しサービス不可通知を提示し(ST84)、一致した場合(ST83; YES)には、エージェント・サーバ2に対し、当該使用者IDと、前述のサービス新規登録の処理で携帯端末1に記入したサービスIDとを送信し(ST85)、以下、当該エージェント・サーバ2において、その使用者ID及びサービスIDのチェック(ST86)及びその判定する(ST87)を行う。

【0129】そして、送信されてきた使用者ID及びサービスIDが不適正なものである場合(ST87; NO)には、当該携帯端末1の利用者に対しサービス不可通知を提示し、それらが適正なものである場合(ST87; YES)には、エージェント・サーバ2は、携帯端末1の使用者へのサービス許可通知及び待機要求(ST88)、並びに携帯端末1の使用者の位置情報の捕捉(ST89)を順次行い、さらに出力情報処理を行った後に(ST90)、その携帯端末1に対し処理終了通知を送信する(ST91)。

【0130】これに対し、携帯端末1では、送信されてきた処理終了通知を表示する(ST92)、続くローカル個人認証(ST93)及びその判別(ST94)並びに個人認証の要求(ST95)については、携帯端末1ではなく、ICカード4において行う。

【0131】そして、エージェント・サーバ2は、携帯端末1に対し処理結果を送信し(ST96)、以下、携帯端末1において、当該処理結果の受信・閲覧表示を行った後に(ST97)、エージェント・サーバ2に受信完了通知を送信し(ST98)、これにより全ての処理を終了する。

【0132】以上、本発明の実施の形態及び実施例につき説明したが、本発明は、必ずしも上述した手段及び手法にのみ限定されるものではなく、本発明にいう目的を達成し、後述する効果を有する範囲内において、適宜、変更実施することが可能なものである。

【0133】

【発明の効果】以上説明したように、本発明によれば、モバイル環境に適応した小型軽量の携帯端末を用いながら、公衆網ネットワークを通じ高度な情報処理を行うことが可能になると共に、高度で占有プログラム容量の大

きい様々なアプリケーションを随意に選択使用することが可能となり、加えて、使用する携帯端末のハードウェア・スペックにつき、将来にわたり陳腐化の問題を生じることがなくなる。

【図面の簡単な説明】

【図1】本発明の実施の形態を示す第1装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【図2】同上における携帯端末及びエージェント・サーバの機能構成を示すブロック図である。

【図3】本発明の実施の形態を示す第2装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【図4】本発明の実施の形態の実施例を示すICカード不要のサービス新規登録の手順を説明するためのフローチャートである。

【図5】同上、サービス環境設定の手順を説明するためのフローチャートである。

【図6】同上、サービス利用の前半の手順を説明するためのフローチャートである。

【図7】同上、サービス利用の後半の手順を説明するためのフローチャートである。

【図8】本発明の実施の形態の実施例を示すICカード要のサービス新規登録の手順を説明するためのフローチャートである。

【図9】同上、サービス環境設定の手順を説明するためのフローチャートである。

*【図10】同上、サービス利用の前半の手順を説明するためのフローチャートである。

【図11】同上、サービス利用の後半の手順を説明するためのフローチャートである。

【符号の説明】

α、β…ネットワーク情報処理システム装置

N…公衆網ネットワーク

1…携帯端末

1a…認証・設定部

10 1b…ネットワーク接続部

11…個人認証手段

12…処理条件設定手段

13…使用者ID/端末ID送信手段

14…処理条件送信手段

15…処理結果受信・閲覧手段

16…処理状況閲覧手段

2…エージェント・サーバ

2a…認証・設定・処理部

20 21…使用者ID/端末ID認証手段

22…判断・処理/機器管理・制御手段

23…処理結果送信手段

24…処理終了通知手段

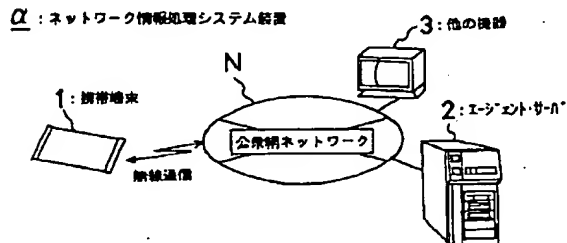
25…端末電源状態監視手段

3…他の機器

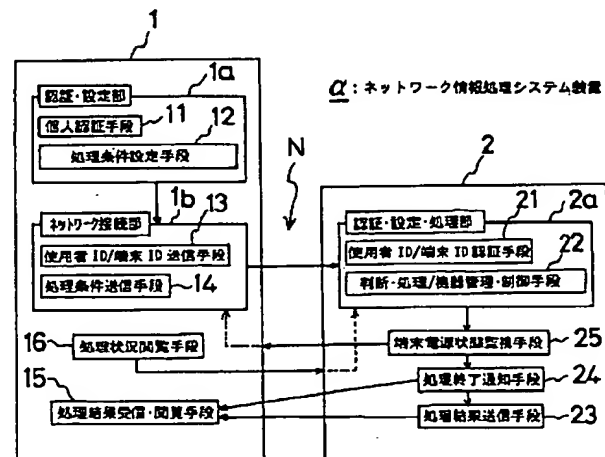
4…ICカード

5…他の端末

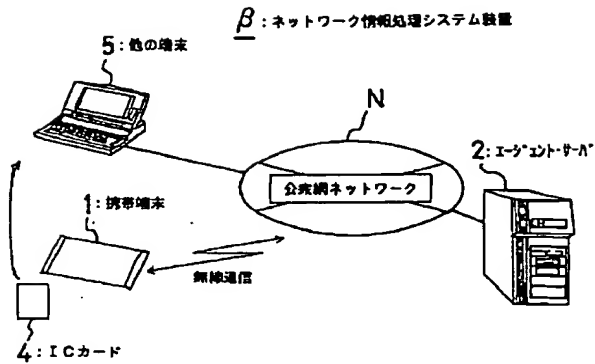
【図1】



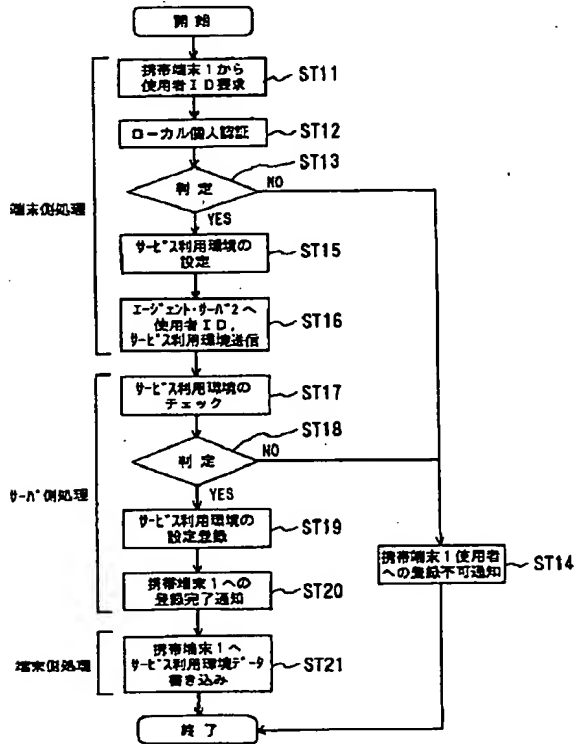
【図2】



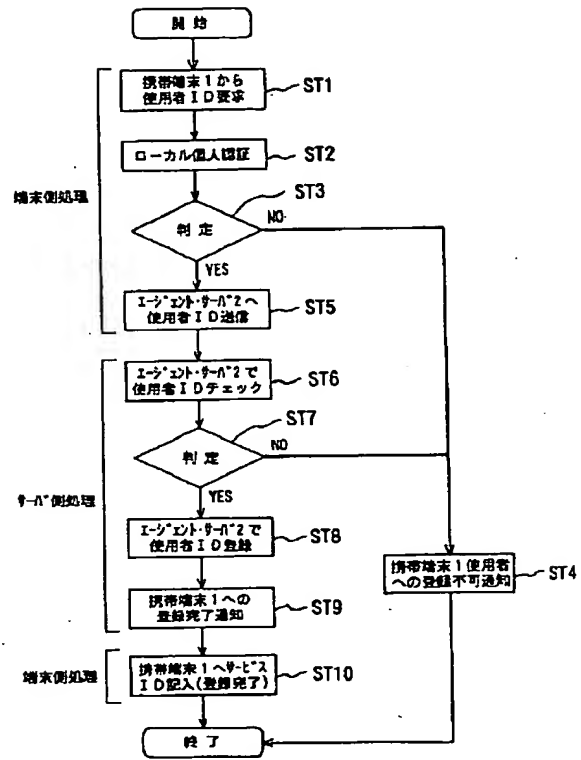
【図3】



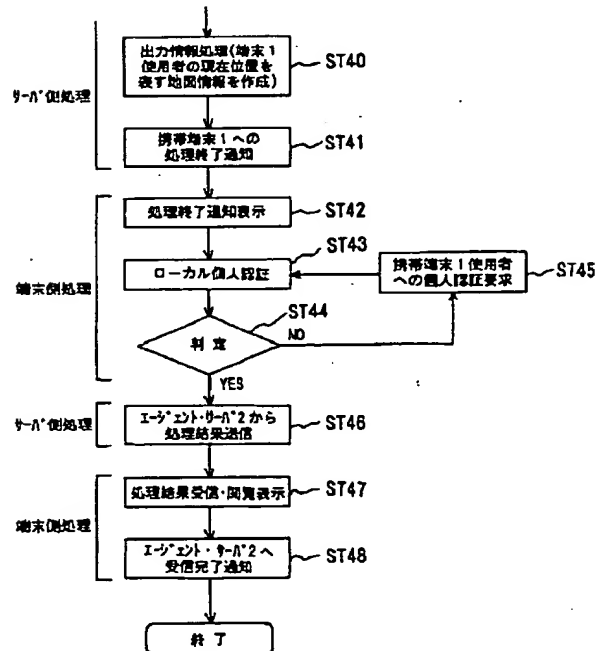
【図5】



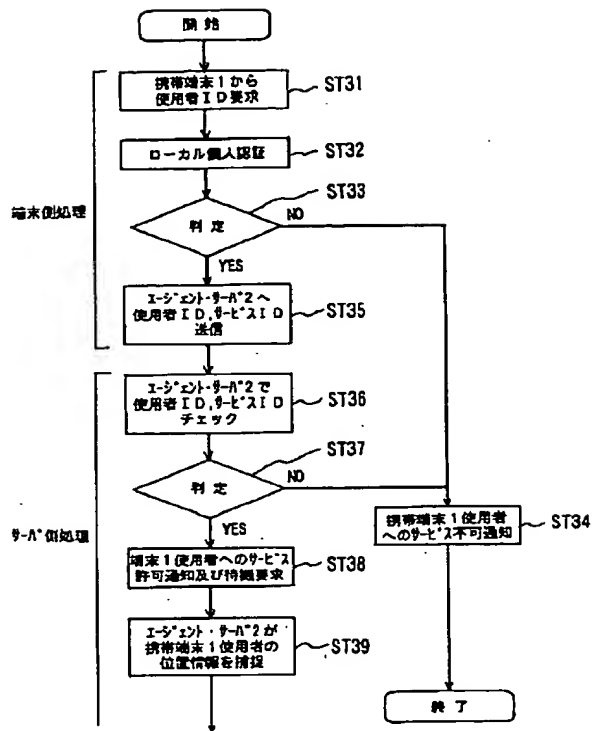
【図4】



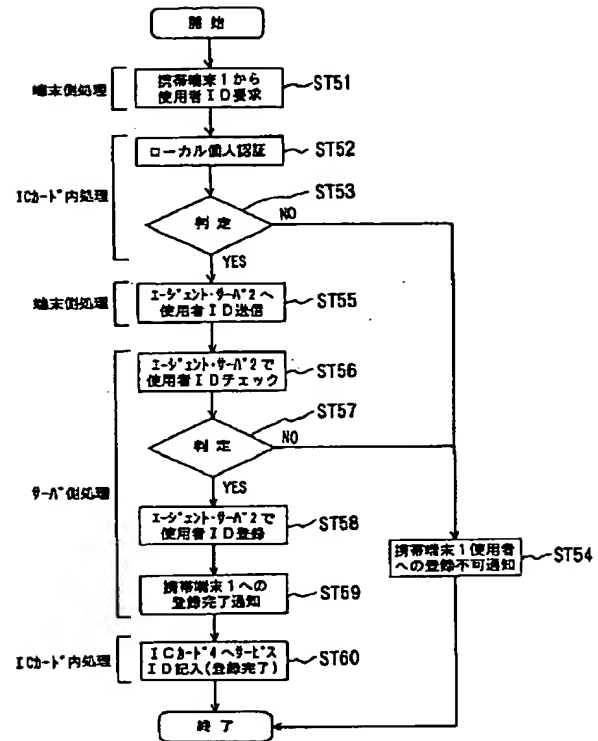
【図7】



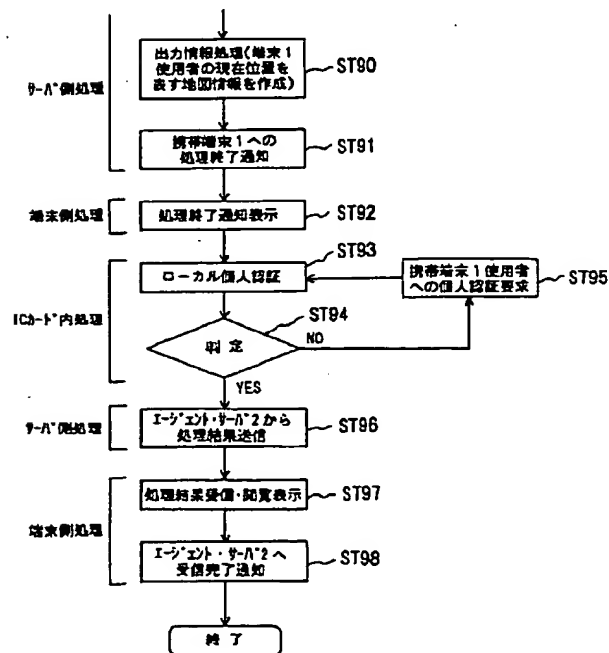
【図6】



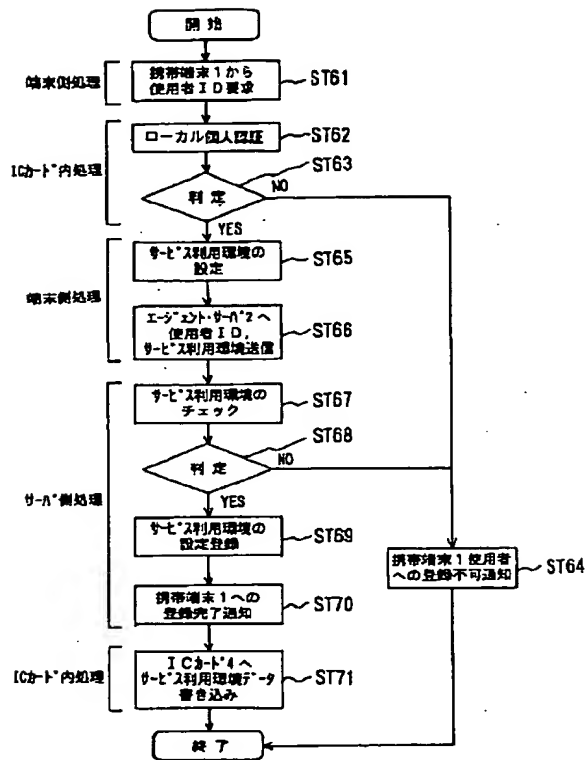
【図8】



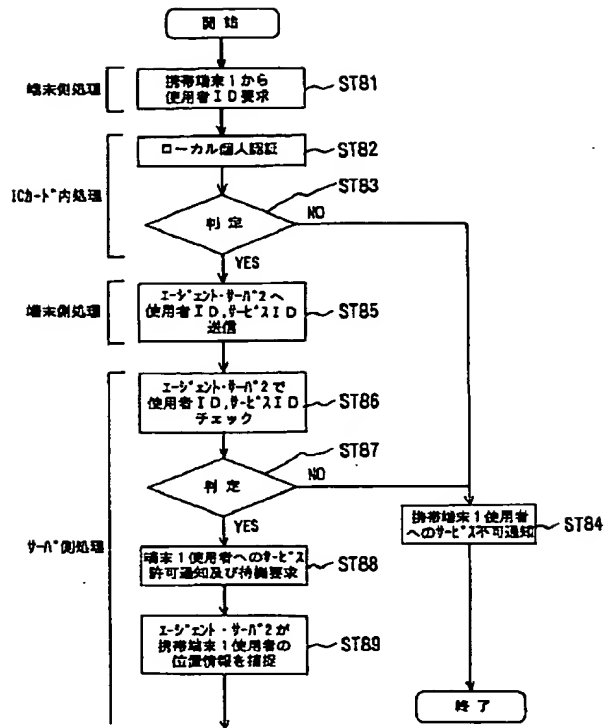
【図11】



【図9】



【図10】



フロントページの続き

(72)発明者 磯村 嘉伯
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 加藤 喜久次
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 酒井 重信
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 斉藤 隆
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 一之瀬 進
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

Fターム(参考) 5B085 AC01 AE01 AE06 AE12 AE23
AE25 BE01 BG07
5B089 AA16 AA22 AB01 AC03 AD11
AE05 BB09